IFW
AP

MS APPEAL BRIEF - PATENTS
PATENT
4450-0305P

IN THE U.S. PATENT AND TRADEMARK OFFICE

In re application of		Before the Board of Appeals	
Han Wah CHIN		Appeal No.:	
Appl. No.:	09/650,254	Group:	2154
Filed:	August 29, 2000	Examiner:	LIN, Kenny
Conf.:	9157		
For:	RELATIVE ADDRESSING FOR NETWORK ELEMENTS		

APPEAL BRIEF TRANSMITTAL FORM

MS APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

August 30, 2004
(Monday)

Sir:

Transmitted herewith is an Appeal Brief (in triplicate) on behalf of the Appellants in connection with the above-identified application.

☐ The enclosed document is being transmitted via the Certificate of Mailing provisions of 37 C.F.R. § 1.8.

A Notice of Appeal was filed on June 29, 2004.

☐ Applicant claims small entity status in accordance with 37 C.F.R. § 1.27

The fee has been calculated as shown below:

☐ Extension of time fee pursuant to 37 C.F.R. §§ 1.17 and 1.136(a) - $0.00.

☒ Fee for filing an Appeal Brief - $330.00 (large entity).

☒ Check(s) in the amount of $330.00 is attached.

☐ Please charge Deposit Account No. 02-2448 in the amount of $0.00. A triplicate copy of this sheet is attached.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By _____
Michael R. Cammarata, #39,491

MRC/JWR/kpc

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000

(Rev. 02/08/2004)

PATENT
4450-0305P

IN THE U.S. PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF		BEFORE THE BOARD OF APPEALS	
Han Wah CHIN		APPEAL NO.:	
APPLN. NO.:	09/650,254	GROUP:	2154
FILED:	August 29, 2000	EXAMINER:	LIN, Kenny
FOR:	RELATIVE ADDRESSING FOR NETWORK ELEMENTS		

BRIEF ON BEHALF OF APPELLANT FILED UNDER PROVISION OF 37 C.F.R. § 1.192

PATENT
4450-0305P

IN RE APPLICATION OF

Han Wah CHIN

Appl. No.: 09/650,254

Filed: August 29, 2000

For: RELATIVE ADDRESSING FOR NETWORK ELEMENTS

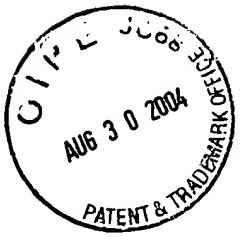
BEFORE THE BOARD OF APPEALS

APPEAL NO.

Group: 2154

Examiner: LIN, Kenny

TABLE OF CONTENTS



PATENT
4450-0305P

IN THE U.S. PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

Applicant:	Hon Wah CHIN	Conf.:	9157
Appl. No.:	09/650,254	Group:	2154
Filed:	August 29, 2000	Examiner:	LIN, Kenny
For:	RELATIVE ADDRESSING FOR NETWORK ELEMENTS		

BRIEF ON BEHALF OF APPELLANT FILED UNDER PROVISION OF 37 C.F.R. § 1.192

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

August 30, 2004
(Monday)

Dear Sir:

This is an Appeal from the Final Rejection of April 8, 2004 of claims 1-21. This Appeal Brief is submitted to support the Notice of Appeal filed on June 29, 2004.

(1) REAL PARTY IN INTEREST:

The named inventors assigned their rights to the invention that is disclosed in the application and any patent that may issue therefrom to ONI SYSTEMS CORP. ONI SYSTEMS CORP. assigned their interest to the invention to CIENA CORPORATION, as recorded in the U.S. Patent and Trademark Office

at Reel 013291, Frame 0660. Thus, CIENA CORPORATION is the real party in interest.

(2) RELATED APPEALS AND INTERFERENCES:

Appellant submits that no other appeals or interferences are known to Appellant, Appellant's legal representative, or the Assignee of the present application, which would directly affect or be affected by, or have a bearing on the Board's decision in the pending Appeal.

(3) STATUS OF THE CLAIMS:

Appellant submits that claims 1-21 are pending in the application. Claims 1, 5, 14, and 18 are independent claims. Claims 1-21 stand rejected and are the claims on Appeal.

(4) STATUS OF ANY AMENDMENT FILED SUBSEQUENT TO FINAL REJECTION:

No amendments were filed after the Final Rejection of April 8, 2004 (Paper No. 11).

(5) SUMMARY OF THE INVENTION:

In conventional packet data networks, each message packet comprises a protocol data unit (PDU) including a message body (payload) and a header. This header contains source and destination address information that other network elements use for forwarding the message packet to its intended

destination. In conventional systems, the address of each node may be assigned at the time the network is designed, or assigned using a configuration process, e.g., a broadcast configuration process in which the nodes negotiate specific node addresses. When a fault occurs disrupting traffic, this type of system must determine the topology of the system, determine the new signal paths, and then negotiate and assign new fixed addresses. Such processing is time consuming, which may result in lost traffic and a limited ability to replace equipment in the network.

The present invention does not require the use of fixed, assigned, or pre-known network addresses. Instead, the present invention is directed to a relative address protocol for sending message packets to a destination node a pre-selected number of nodes away from the source node along a portion of a network. The relative address protocol may be used along any portion of a network, which acts or behaves as a linear chain of nodes connected by data links (e.g., as illustrated in Fig. 5). In other words, the protocol may be used for linear chain networks, any portion of a network that functions as a chain network, or virtual chain networks (Specification at page 14, line 8-16).

Fig. 4 illustrates the relative address protocol 400. Message packets using this protocol include a header portion 490, which contains a relative destination address field 420 and a relative source address field 430. The relative destination address field further contains a counter 440. The header 490 may further include an identifier 410 that identifies that the relative address protocol is implemented in the packet (Spec. at page 11, lines 8-9).

Fig. 5 illustrates an example of using the relative address protocol 400. The counter 440 of the relative address protocol 400 is configured to count the number of nodes that the message packet has encountered (i.e., "hopped") since being transmitted from its source node 505 (Spec. at page 10, lines 14-16). The relative source address field 430 records the number of node hops that the message packet must travel from the source node 505 to reach the destination node 520. The counter 440 is either incremented or decremented in value by a desired step at each new node that the message packet encounters (Spec. at page 12, lines 13-14). When the counter 440 reaches a trigger value, the message packet has performed the predetermined number of hops (Spec at page 12, lines 3-8). The nodes are programmed so that the message packet is accepted by the node at which the message packet's counter reaches the trigger value (Spec. at page 12, lines 14-17).

For example, in a countdown mode, the source node 505 may initialize the counter 440 with the value of the desired number of node hops. Such an example is illustrated in Fig. 5. Thereafter, the counter may be decremented by a value of one at each node. The trigger value is set for the value of zero. In other words, the node 520 at which the counter 440 is decremented to zero will accept the message packet. Spec. at page 13, line 19 – page 14, line 7.

Alternatively, a count up mode may be used in which the counter 440 is initialized at a value of zero, and incremented by a value of one at each encountered node. The trigger value may equal the pre-selected number of

node hops to the destination node (i.e., the value in the relative source address field 430). Spec. at page 12, line 20 – page 13, line 8.

The value in the relative address field allows the destination node 520 to determine a relative return address of the source node 505. For example, a first message packet may be sent in one direction of the chain network to a destination node 520. After accepting the message packet, the destination node 520 may use the value in the relative source address field 430 to determine the pre-selected number of hops for sending a reply message packet (in the opposite direction) to the source node 505. Spec. at page 12, lines 5-8.

(6) ISSUES PRESENTED

A. Whether claims 1-8, 10, 11, 14, and 18 are unpatentable under 35 U.S.C. § 102 over Melnik.

B. Whether claims 9, 12, 13, 15-17, and 19-21 are unpatentable under 35 U.S.C. § 103 over Melnik.

Appellant respectfully submits that the answer to each of these issues is in the negative.

(7) GROUPING OF CLAIMS

For purpose of this appeal, Appellant groups the claims as follows:

I: Independent claim 1 stands or falls together with its dependent claims 2-4.

II: Independent claim 5 stands or falls together with its dependent claims 6-13.

III: Independent claim 14 stands or falls together with its dependent claim 21.

IV: Independent claim 18 stands or falls by itself.

V: Claim 19 does not stand or fall with its base claim 18. Claim 20 stands or falls together with claim 19.

(8) ARGUMENTS

A. The Rejection of Claims 1-8, 10, 11, 14, and 18 Under 35 U.S.C. § 102.

Claims 1-8, 10, 11, 14, and 18 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Melnik.

1. Summary of the Examiner's Rejection

With respect to claims 1-8, 10, 11, 14, and 18, the Examiner asserts that Melnik discloses an address protocol for forwarding a message packet from a source node to a destination node, along a sequence of communicatively coupled nodes functioning as a linear chain network, referring to col. 6, lines 61-67; and col. 7, lines 1-11. *See* Paper No. 11 at § 5, page 3.

The Examiner asserts that Melnik discloses a relative destination address field including a counter, referring to col. 7, lines 2-19. The Examiner also asserts that Melnik discloses programming the counter with an initial value corresponding to a destination node, which is a pre-selected number of nodes away from the source node along the linear chain network, referring to col. 3, lines 29-36; and col. 13, lines 33-35. *See* Paper No. 11 at § 5.a, page 3.

The Examiner further asserts that Melnik teaches that the counter is adjusted by a pre-selected step in value at each node. The Examiner further asserts that Melnik discloses that the message packet is forwarded along the chain network until the counter reaches a trigger value, which indicates that the destination node has been reached. For the above assertions, the Examiner refers to Melnik at col. 3, lines 29-36; col. 7, lines 2-8; and col. 17, lines 1-4. *See* Paper No. 11 at § 5.b, page 3.

The Examiner further asserts that Melnik discloses that the destination node does not require address information, in addition to the counter reaching the trigger value, to accept the message packet. For this assertion, the Examiner refers to Melnik at col. 3, lines 29-36. *See* Paper No. 11 at § 5.c, page 3.

2. The Teachings of Melnik

Melnik teaches that conventional network routing protocols, which are used in wireless, multihop networks include two main categories: random routing protocols, and deterministic routing protocols. *See, e.g.*, col. 3, lines 16-19.

In col. 3, lines 20-58, Melnik describes prior art networks that use the conventional random routing protocol. In such networks, Melnik teaches that data packets are "randomly hopped through the nodes in the network from a sender node to a destination node along random routes, with **no specific set of repeater[nodes] being used** to effect the data transfer" (col. 3, lines 20-24;

emphasis added). Melnik specifically discloses the operation of these networks as follows. Each transmitted packet includes a hop counter, which is set by the sender node. The sender node transmits the packet to all nodes within a transmitting range. Each node receiving the packet decrements the hop counter. Then, each receiving node will retransmit the packet to every node in its range, and so on, with two exceptions. The packet will not be repeated if: the receiving node is the destination node, or if the packet has dominated network resources for too long. If the receiving node is the destination node (based on a comparison of address information), it returns an acknowledgement packet. *See* col. 3, lines 24-36 and 48-50.

Although Melnik does not expressly disclose how the random protocol determines whether the receiving node is the destination node, nothing in Melnik suggests using any other method than the conventional method of examining address information in the packet.

In the random routing protocol, Melnik discloses that the sender node will set the hop counter of the packet at a value, "such that the **probability that the packet reaches the destination is maximized, without dominating the** network for an unduly length of time" (col. 3, lines 32-36; emphasis added).

Melnik discloses that the prior art random routing networks have a significant drawback in that there is a high probability that most, in not all, nodes in the network will handle every transmitted packet. This significantly

increases the data traffic density, and limits the amount of different packets that can be transmitted on the network at a given time. *See* col. 3, lines 37-43.

With respect to the conventional deterministic routing protocols, Melnik teaches that packets are transmitted and relayed to each particular node using a single chain of nodes. Melnik teaches that a significant drawback of such networks is the requirement that each node have sufficient memory and processing capabilities to implement routing tables to make the routing decisions for each packet. *See* col. 3, line 59 – col. 4, line 20.

Melnik discloses a system and protocol designed to overcome the drawbacks of the conventional protocols. Specifically, Melnik discloses a wireless, multihop network 20 that is organized into multiple bands of nodes 22. Melnik discloses that each band is comprised of nodes 22 that are located the same number of hops from a control node 24. Melnik further teaches that each node 22 is assigned to a chain of nodes for purposes of receiving and relaying packets. Furthermore, a logical Partitioned Spanning Tree (PaST) address is assigned to each node 22. The logical address of each node identifies the chain to which it belongs. *See, e.g.*, col. 8, line 55 – col. 9, line 34; and Fig. 2.

Specifically, Melnik teaches that each logical PaST address assigned to a particular node includes a plurality of segments, each segment corresponding to one of the bands in that particular node's chain. Each segment in the logical address uniquely identifies a node within the corresponding band, which belongs to the same chain. For example, a destination node may be

assigned a logical address of "0100/011/11/011," which identifies the chain to the destination node. The first segment "0100" identifies the node in the destination node's chain, which is located in the first band. The segments "011" and "11" identify the nodes in that chain, which are located in the second and third bands, respectively. The last segment "011" uniquely identifies the destination node from the other nodes in the fourth band. *See* col. 9, line 43 – col. 10, line 15.

Melnik discloses that each transmitted packet includes a LOGICAL ADDRESS field containing the PaST address of the destination node. Melnik's packet also contains a HOP field, which includes the designated number of hops for the packet (first half of field) and a counter (second half of field). *See, e.g.*, col. 10, lines 52-62; col. 13, line 24 – col. 14, line 9; and Fig. 4.

According to Melnik, after a node transmits a packet, each node in the subsequent band receives and processes the packet. This processing requires each node to increment the packet's counter (second half of HOP) and compare it to the packet's designated number of hops (first half of HOP field) in the packet. If the counter has not reached the designated number, the node **compares its own unique identifier** (last K bits of its own logical PaST address) **with the corresponding segment in the packet's destination address** (LOGICAL ADDRESS) to determine whether the node is in the same chain as the destination node. If the node's unique identifier matches the segment, the node will relay it to the next band. *See, e.g.*, col. 13, line 62 – col. 14, line 59; Figs. 3 and 4.

However, if the node determines that the counter has reached the designated number of hops, each node within that band compares its unique identifier with the relevant segment **in the destination address**. Melnik discloses that the destination node is the one whose unique identifier **matches this segment in the destination address**. *See Id.*

3. Rejection of Claims 1 and 5 Under 35 U.S.C. § 102 is Improper.

As set forth in Section 2131 of the MPEP Original Eighth Edition, August, 2001, page 2100-68:

> "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. V. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claims." *Richardson v. Suzuki Motor Co.*, 868 F2d 1226, 1236, 9 USQP2d 1913, 1920 (Fed. Cir. 1989).

Independent claims 1 and 5 recite an address protocol for forwarding message packets from a source node to a destination node along nodes "functioning as a linear chain network," in which a counter is "programmed with an initial value at the source node corresponding to a destination node that is a preselected number of nodes away the source node along the linear chain network." Also, in claims 1 and 5, "the destination node does not require address information in addition to the counter reaching the trigger value to accept the message packet." These features are not disclosed by Melnik for the reasons discussed herein.

a. Examiner Impermissibly Combines Different Inventions in the § 102 Rejection.

Initially, Appellant points out that the Examiner's rejection relies on portions from the BACKGROUND OF THE INVENTION, and the SUMMARY OF THE INVENTION and DETAILED DESCRIPTION OF THE INVENTION in Melnik to provide teachings to anticipate the present invention. *See*, e.g., Paper No. 11 at §§ 5-6, pages 3-4.

For example, with respect to claim 5, the Examiner relies on col. 7, lines 9-10 (in Melnik's SUMMARY) and col. 8, lines 27-33 (in Melnik's DETAILED DESCRIPTION) to teach the claimed identifier field, while concurrently relying on col. 3, lines 29-36 (in Melnik's BACKGROUND) to disclose that a destination node accepts a message packet without requiring address information in addition to the counter reaching the trigger value. *See* Paper No. 11 at § 6.a – § 6.d, pages 3-4.

Appellant respectfully submits that the protocol in col. 3, lines 29-36 of Melnik's BACKGROUND is **a separate and distinct invention** from the protocol, which is disclosed as Melnik's invention in the SUMMARY and DETAILED DESCRIPTION. Thus, the Examiner is attempting to combine **completely different inventions** to anticipate the claims under § 102. Specifically, the protocol referred to in Melnik's BACKGROUND uses a random routing algorithm in which data packets are sent from a sender to a destination along random routes (*see, e.g.*, col. 3, lines 20-24), while Melnik's invention

assigns each node to a chain of nodes through for the purposes of receiving and relaying packets (*see, e.g.*, col. 9, lines 15-23). These are completely different protocols and, thus, cannot be treated as one invention for purposes of 35 U.S.C. § 102.

Furthermore, Melnik teaches away from using the random routing protocol in the BACKGROUND. Specifically, Melnik points out that increased traffic density is a significant drawback of random routing protocols. *See, e.g.*, col. 3, lines 37-46. Melnik further discloses that there is a need for overcoming the shortcomings of such prior art protocols in col. 6, lines 24-35.

Furthermore, Appellants respectfully submit that the Examiner, in making this rejection, has failed to consider the portions of Melnik teaching away from the random routing protocol because of its drawbacks. Thus, even assuming that the random routing protocol teaches some elements in the claimed invention, the Examiner has failed to consider the portions of Melnik that **teach away** from such elements (i.e., by teaching away from the random protocol). As set forth in MPEP § 2141.03, "[a] prior art reference must be considered in its entirety, including disclosures that teach away from the claimed invention. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 7220 USPQ 303 (Fed. Cir. 1983)."

b. The Random Routing Protocol in Melnik's BACKGROUND Fails to Teach Every Element in Claims 1 and 5.

Initially, Appellant points out that, in the random routing protocol described in Melnik's BACKGROUND, each node sending or relaying a packet

does so by transmitting the packet **to all nodes in its transmitting range**. *See,* col. 3, lines 24-28. Accordingly, the nodes using such random routing protocols **do not function as a linear chain network**, as required by claims 1 and 5. In networks functioning as linear chain networks, a node will send or relay a packet only to the subsequent node in the pre-selected chain of nodes during each hop. *See, e.g.*, Spec. at page 14, lines 8-16.

In the rejection of each of independent claims 1 and 5 the Examiner asserts that the random routing protocol in Melnik's BACKGROUND to teach that "the destination node does not require address information in addition to the counter reaching the trigger value to accept the message packet."

Furthermore, the hop counter in each packet of the random routing protocol is set "such that the probability that the packet reaches the destination node is maximized, without dominating the network for an unduly length of time." *See* col. 3, lines 32-35. Thus, the initial value of the random routing protocol's hop counter **does not correspond to the number of nodes separating the sender and destination nodes** (as required by claims 1 and 5). In fact, since the packet is being transmitted along random routes, with no specific set of repeaters being used (*see* col. 3, lines 20-24), **there is no way of knowing how many hops are required to reach the destination node** in the random routing protocol.

Furthermore, in the random routing protocol, Melnik expressly teaches that the initial value of the hop counter is set so that "the probability that the packet reaches the destination node is maximized, without dominating the

network resources for an unduly length of time" (col. 3, lines 32-35). Thus, when this hop counter reaches the trigger value (of zero), this merely indicates that the **packet has dominated network resources too long and should no longer be relayed**. As such, the fact that the hop counter reaches the trigger value **does not indicate that the destination node has been reached** in the random routing protocol.

Therefore, it is clear that, in the random routing protocol in Melnik's BACKGROUND, each node that receives a message packet cannot rely on the value of the hop counter to determine whether it is the destination node. Each receiving node is implicitly required to compare address information in the packet with the node's own address to determine whether it should accept the packet (as the destination node), or relay the packet to other nodes.

However, by asserting that the destination node of the random protocol does not require address information to accept the packet, the Examiner apparently confuses the destination node's operation with that of a node that merely receives and retransmits the packet. However, in order for the destination node to **accept** the packet, instead of merely **relaying** the packet, it is clear that **the random routing protocol requires the destination node to compare address information in the packet with its own address.**

c. The Protocol in Melnik's SUMMARY/DETAILED DESCRIPTION Fails to Teach Every Element in Claims 1 and 5.

According to the network and protocol, which is the subject of Melnik's invention, the destination node will only accept a packet if two conditions are

met: 1) the counter is equal to the designated number of hops; and 2) a last segment of the packet's destination address matches the unique identifier of the destination node. *See, e.g.*, col. 14, lines 48-59. In fact, Melnik discloses that each intervening node in the destination node's chain will accept a packet, for purposes of relaying the packet, only if a segment in the packet's destination address (corresponding to the intervening node's band) matches the intervening node's unique identifier. *See* col. 13, line 62 – col. 14, line 47.

Thus, according to the protocol of Melnik's invention, the destination node **requires address information** to determine whether to accept a message packet.

d. Melnik Fails to Anticipate Claims 1 and 5.

Neither the random protocol in Melnik's BACKGROUND, nor the protocol in Melnik's SUMMARY/DETAILED DESCRIPTION, provides a teaching that "the destination node does not require address information in addition to the counter reaching the trigger value to accept the message packet," as required by claim 1. Furthermore, claims 2-4 incorporate this feature by virtue of its dependency on claim 1.

Furthermore, it is respectfully submitted that claim 5 recites that the destination node "does not require address information in addition to the counter reaching the trigger value to accept the message packet." Also, claims 6-8, 10, and 11 incorporate this feature by virtue of their dependency on claim 5. Since none of the protocols described by Melnik disclose this feature, it is

respectfully submitted that the rejection claims 1-8, 10, and 11 under 35 U.S.C. § 102 is improper and should be reversed.

4. The Rejection of Claims 14 and 18 Under 35 U.S.C. § 102 is Improper.

Furthermore, independent claim 14 recites a method of sending packets along nodes functioning as a chain network, which includes "accepting the message packet at a destination node... without requiring address information in addition to the counter reaching the rigger value to accept the message packet."

Also, independent claim 18 recites a method of sending packets along a chain network, which includes "accepting the message packet at a destination node... without requiring address information in addition to the counter reaching the trigger value to accept the message packet."

At least for the reasons set forth above in connection with claims 1 and 5, Appellant respectfully submits that the random routing protocol in Melnik's BACKGROUND does not disclose nodes that function as a chain network, or that a destination node accepts a packet without using address information. Also, as discussed above with regard to claims 1 and 5, the protocol disclosed in Melnik's SUMMARY/DETAILED DESCRIPTION expressly uses address information in determining whether the destination node accepts the packet.

As such, the above features in claims 14 and 18 are not disclosed by either the random routing protocol in Melnik's BACKGROUND or the protocol in Melnik's SUMMARY and DETAILED DESCRIPTION. Thus, it is respectfully

submitted that the rejection of claims 14 and 18 under 35 U.S.C. § 102 is improper and should be reversed.

B. The Examiner's Rejection of Claims 9, 12, 13, 15-17 and 19-21 under 35 U.S.C. § 103 over Melnik

Initially, Appellant points out that MPEP § 2141 requires that the following factual inquiries, as set forth in *Graham v. John Deere*, 148 USPQ 459 (1966), be applied in each and every rejection under 35 U.S.C. § 103:

(A) Determining the scope and contents of the prior art;

(B) Ascertaining the differences between the prior art and the claims in issue;

(C) Resolving the level of ordinary skill in the pertinent art; and

(D) Evaluating evidence of secondary considerations.

Appellant respectfully submits that, in view of the § 102 rejection of claims 1 and 5, it is clear that the Examiner has failed to properly determine the scope and contents of the prior art. Specifically, the Examiner by attempting to combine the random routing protocol in Melnik's BACKGROUND with the protocol in Melnik's SUMMARY/DETAILED DESCRIPTION, the Examiner has apparent failed to recognize that these protocols **are distinct and separate inventions**.

Furthermore, it is respectfully submitted that the Examiner has given no indication in § 103 rejection of claims 9, 12, 13, 15-17 and 19-21 that the Examiner has correctly determined the scope or content of the distinct inventions disclosed in Melnik. In particular, the Examiner has made no

attempt to provide a teaching, suggestion, or motivation for combining the protocol in Melnik's BACKGROUND and the protocol in Melnik's SUMMARY/DETAILED DESCRIPTION, as required for a obviousness rejection in which separate inventions are combined. *See, e.g.*, MPEP § 2143.

Furthermore, even assuming that the Examiner had provided a proper teaching or motivation to combine the protocol of Melnik's BACKGROUND with the protocol in Melnik's SUMMARY/DETAILED DESCRIPTION, Appellant respectfully submits that the resultant combination would be insufficient under § 103 because of its vast differences in structure and operation with respect to the claimed invention.

Since the Examiner has failed to properly follow the analysis of *Graham v. John Deere*, at least for the reasons set forth above, it is respectfully submitted that the rejection of claims 9, 12, 13, 15-17 and 19-21 is improper and should be reversed.

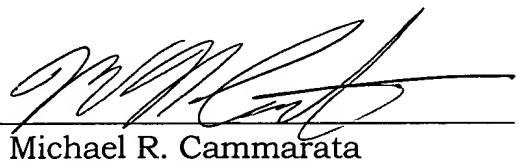
(9) CONCLUSION

For the reasons advanced above, it is respectfully submitted that all the claims in this application are allowable. Thus, favorable reconsideration and reversal of the Examiner's Final Rejection of claims 1-29 by the Honorable Board of Patent Appeals and Interferences, is respectfully requested.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Very truly yours,

BIRCH, STEWART, KOLASCH & BIRCH

By 

Michael R. Cammarata
Reg. No. 39,491

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000

MRC/JWR

(9) APPENDIX OF CLAIMS

Claim 1. An address protocol for forwarding a message packet from a source node to a destination node along a sequence of communicatively coupled nodes functioning as a linear chain network, the address protocol comprising:

a relative destination address field including a counter programmed with an initial value at the source node corresponding to a destination node that is a preselected number of nodes away from the source node along the linear chain network;

wherein the counter is adjusted by a preselected step in value at each node the message packet is forwarded to along the chain network until the counter reaches a trigger value indicating that the destination node has been reached, and

wherein the destination node does not require address information in addition to the counter reaching the trigger value to accept the message packet.

Claim 2. The protocol of Claim 1, further comprising an identifier field containing an identifier to identify the message packet as having a relative address protocol.

Claim 3. The protocol of Claim 2, further comprising a relative source destination field containing the initial value.

Claim 4. The protocol of Claim 1, further comprising a relative source destination field containing the initial value.

Claim 5. An address protocol for forwarding a message packet from a source node to a destination node along a sequence of communicatively coupled nodes functioning as a linear chain network, the address protocol comprising:

an identifier field containing an identifier to identify the message packet as having a relative address protocol; and

a relative destination address field including a counter programmed with an initial value at the source node corresponding to a destination node that is a preselected number of nodes away from the source node along the linear chain network;

wherein the counter is adjusted by a preselected step in value at each node the message packet is forwarded to along the linear chain network until the counter reaches a trigger value indicating that the destination node has been reached, and

wherein the destination node does not require address information in addition to the counter reaching the trigger value to accept the message packet.

Claim 6. The protocol of Claim 5, further comprising a relative source address field for storing the initial value.

Claim 7. The protocol of Claim 5, wherein the initial value is an integer having an absolute value equal to the desired number of node hops and the counter is changed by a step in value of one at each node.

Claim 8. The protocol of Claim 7, wherein the counter is programmed with the initial value and the counter is counted down by one at each node hop until a trigger value of zero is reached.

Claim 9. The protocol of Claim 7, wherein the counter has an initial value of zero and the counter is counted up by one at each node hop until a trigger value equal to the initial value is reached.

Claim 10. The protocol of Claim 5, wherein the initial value is a linear function of the desired number of node hops.

Claim 11. The protocol of Claim 5, wherein at least one node in the linear chain is a regenerator element.

Claim 12. The protocol of Claim 5, wherein the chain network is a virtual chain network.

Claim 13. The protocol of Claim 5, wherein the chain network comprises a portion of a ring network.

Claim 14. A method of sending a message packet along a portion of a network functioning as a linear chain network from a source node to a destination node using an address protocol having an identifier to identify the message packet as having a relative address protocol, a relative source address field for storing an initial value, and a relative destination address field containing a counter, the method comprising the steps of:

selecting an initial value that is a function of a desired number of node hops along the linear chain network from the source node;

programming the counter to have the initial value;

adjusting the counter by a preselected step in value at each node that the message packet is forwarded to; and

accepting the message packet at a destination node when the counter value reaches a preselected trigger value without requiring address information in addition to the counter reaching the trigger value to accept the message packet;

wherein the preselected step in value is chosen so that the counter reaches the trigger value when the packet has completed the desired number of node hops.

Claim 15. The method of Claim 14, wherein the message packet comprises a status query message and further comprising the steps of:

requesting the destination node to send a status message packet having a second identification field and a second counter in a direction along the chain back to the source node;

programming the second counter to have the initial value;

adjusting the second counter by the preselected step in value at each node that the message packet is forwarded to; and

accepting the status message packet when the counter reaches the preselected trigger value;

whereby the status message packet is returned to the source node.

Claim 16. The method of Claim 15, wherein at least one of the nodes of the chain includes a regenerator element.

Claim 17. The method of claim 15, further comprising the steps of:

selecting a return message;

programming a second counter disposed in an address protocol of the return message to have a return value having equal magnitude of the initial value;

transmitting the second message in the return direction;

adjusting the second counter by the magnitude of the preselected value at each node that the message packet is forwarded to; and

accepting the return message packet at the source node when the second counter reaches the preselected trigger value.

Claim 18. A method of sending a message packet along a chain network having regenerator nodes from a source node to a destination node using an address protocol having an identifier to identify the message packet as having a relative address protocol, a relative source address for storing an initial value, and a relative destination address field containing a counter, the method comprising the steps of:

selecting an initial value that is a function of a desired number of node hops along the linear chain from the source node;

programming the counter to have the initial value;

adjusting the initial value of the counter by a preselected step in value at each node that the message packet is forwarded to; and

accepting the message packet at a destination node when the counter value reaches a preselected trigger value without requiring address information in addition to the counter reaching the trigger value to accept the message packet;

wherein the preselected step in value is chosen so that the initial value reaches the trigger value when the packet has completed the desired number of node hops.

Claim 19. The method of Claim 18, wherein the message packet comprises a status query message and further comprising the steps of:

requesting the destination node to send a status message packet having a second identification field and a second counter back to the source node;

programming the second counter to have the initial value;

adjusting the second counter by the preselected step in value at each node that the message packet is forwarded to; and

accepting the message packet when the second counter reaches the preselected trigger value;

whereby the status message packet is returned to the source node.

Claim 20. The method of Claim 19, further comprising the steps of:

sending a plurality of status query messages to a plurality of destination nodes, the destination nodes having initial values corresponding to nodes that are each a different number of node hops from the source node;

receiving status messages from responding destination nodes; and

determining the relative distance of responding nodes as a function of the initial value of each responding node;

whereby a fault is isolated to a part of the network subsequent to the responding active node the greatest number of node hops from the source node.

Claim 21. The method of Claim 14, further comprising the step of:

detecting a fault in a linear chain of regenerator nodes using the relative address protocol by:

sending a first status query message packet requesting a return status message from a destination node at least one node hop from the source node; and

sending at least one subsequent status query message packet requesting a return status message from another destination node corresponding to a different number of node hops from the source node and recording whether the return status message is received at the source node; and

determining the node the greatest number of node hops from the source node replying to the status query message directed to it;

wherein a fault is isolated to a portion of the chain network subsequent to the node the greatest number of node hops from the source node returning the corresponding status message.